A LEGAL AND LAW ENFORCEMENT GUIDE TO TELEPHONY

ABOUT THE AUTHOR

George Molczan is Director of Network Services for General Communication, Inc. (GCI) in Anchorage, Alaska. In addition to his responsibilities for the operation and maintenance of GCI's switched network, he is responsible for compliance with court orders, subpoenas, and search warrants from attorneys and law enforcement agencies and frequently testifies regarding telephony issues.

George's career includes a broad range of technical and managerial experience with Pacific Northwest Bell (now part of Qwest) as well as GCI. His diverse background makes him comfortable discussing corporate budgets or explaining call routing, installing trap and trace devices, and discussing telephony-related legislation. He can be reached by e-mail at george@gmolczan.com.

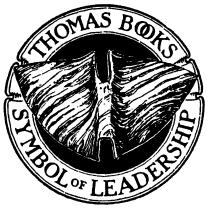
A LEGAL AND LAW ENFORCEMENT GUIDE TO TELEPHONY

Addressing Technical, Legal and Police Issues Relating to the Interface and Interaction with Communication Service Providers

By

GEORGE MOLCZAN

Director, Network Services–Operations
General Communications, Inc.
Anchorage, Alaska



CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

ISBN 0-398-07574-3
ISBN 0-398-07575-1

Library of Congress Catalog Card Number: 2004062067

With THOMAS BOOKS *careful attention is given to all details of manufacturing and design. It is the Publisher's desire to present books that are satisfactory as to their physical qualities and artistic possibilities and appropriate for their particular use.* THOMAS BOOKS *will be true to those laws of quality that assure a good name and good will.*

Printed in the United States of America
CR-R-3

Library of Congress Cataloging-in-Publication Data

Molczan, George.
A legal and law enforcement guide to telephony : addressing technical, legal and police issues relating to the interface and interaction with communication service providers / by George Molczan.
p. cm.
Includes index.
ISBN 0-398-07574-3 -- ISBN 0-398-07575-1 (pbk.)
1. Telephone companies--United States. 2. Telephone--United States. 3. Telephone companies--Corrupt practices--United States. 4. Telephone--Law and legislation--United States. 5. Law enforcement--United States. 6. Electronic surveillance--United States. I. Title.

HE8815.M65 2005
384.3'02'43632--dc22

2004062067

PREFACE

A *Legal and Law Enforcement Guide to Telephony* addresses technical and legal issues relating to attorney and law enforcement's interface and interaction with communication service providers. The goal is to provide legal and law enforcement practitioners with factual, informative, and easy-to-understand information about telephone company interworkings, their networks, and operation. The range of subjects includes local, long distance, and cellular services; private phone systems (PBX and KTS); 911 systems; telephone fraud; pay phones; customer premises wiring; and new technologies including voice over the Internet (VoIP).

Telephone calls, like people, leave fingerprints known as *call records* for virtually every call that passes through the telephone network. These fingerprints are useful to law enforcement, aiding in reconstructing events and tracking the movement of individuals. Although competition in the local, long distance, and cellular industries has increased the need to generate a greater volume of call records, the typical subpoena does not result in an exhaustive discovery. Many telephone company personnel are unaware that some of these records exist, where they are, or how to find them. Unlike investigations where trained law enforcement specialists look for and gather evidence, law enforcement agencies are dependent on telephone company personnel to look for and gather call records. Armed with the knowledge presented here, investigators will be prepared to probe the innerworkings of telephone companies guiding the search for evidence.

It is not the intent of the author, the publisher, or the sellers of this text to provide legal guidance nor do they claim to be qualified to do so. While this text discusses various technical aspects of monitoring the telephone network or a subscriber's telephone line, the author,

publishers and sellers make no representation of the legality of these practices. The reader is advised to seek legal counsel in regard to any and all monitoring of any portion of the telephone network or requesting or application of information received from a communication service provider.

CONTENTS

TABLES

Page

A LEGAL AND LAW ENFORCEMENT GUIDE TO TELEPHONY

Chapter 1

THE TELCO AND THE LAW

Living in an era when consumer privacy issues are of foremost concern to many people makes savvy businesses sensitive to privacy issues. Consumer information including name, address, account number, and payment information is just a part of the privacy issue for telephone companies. Directory listings and call records detailing calls made and when are also major issues. This chapter covers the relationship issues between communication service providers and law enforcement agencies.

1.1 LAW ENFORCEMENT AND TELEPHONE SERVICE PROVIDERS

Several options are available for gathering information about or from a subscriber line. This section covers subscriber information, traps/traces, and physical monitoring of a subscriber line and the various technical and legal issues.

1.1.1 Traps and Traces Conducted by Service Providers

When a local service provider places a trap on a telephone line (known as the target line) it can be as simple as activating *call detail recording* for the target line. Detailed call recording forces a call detail record (CDR) to be generated for every call to and from a line, including partial dials for outgoing calls. This type of trap provides calling information that includes originating and terminating telephone numbers for incoming and outgoing calls, date, and time. Activation of this type of trap starts generation and collection of CDR information. United States Code, Title 18, Part II, Chapter 206, Pen Registers and

Trap and Trace Devices," includes the following definition of a trap and trace device:

> Section 3127 defines "trap and trace device" as a device or process which captures the incoming electronic or other impulses which identify the originating number of other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

Individual telephone companies have different policies for placing a trap on a line. For some it is a written request from a law enforcement agency (LEA) while for others a subscriber request is sufficient. Unless otherwise requested by a LEA, traps are set to collect call data for 30 days. In some cases telephone companies charge the subscriber for placing a trap on their line. In any case, the CDRs generated by the trap are only released to a LEA when the LEA produces the proper documentation in the form of a warrant, subpoena, or court order.

Requests for a trap and trace based on an immediate requirement, such as catching someone in the act of making a threatening call, typically require a court order. Telephone companies handle these as special cases with call trap data being sent directly to a network operations center that is in direct contact with the LEA.

1.1.2 Physical Monitoring of a Subscriber Line

There are three ways to physically monitor an analog subscriber line:

- Pen Registers–Trap and trace device
- Wiretaps
- CALEA

Pen registers, also known as trap and trace devices,[1] bridge onto the target line at a telephone company main distribution frame or other analog cross-connect point. The cross-connect point could be in a central office, a remote wire center or at a digital loop carrier (DLC) field

1. United States Code, Title 18, Part II, Chapter 206, Section 3127 describes the use and placement of pen registers.

installation. Figure 1.1 shows the pen register connection points, all of which are mainframes or cross-connect frames.

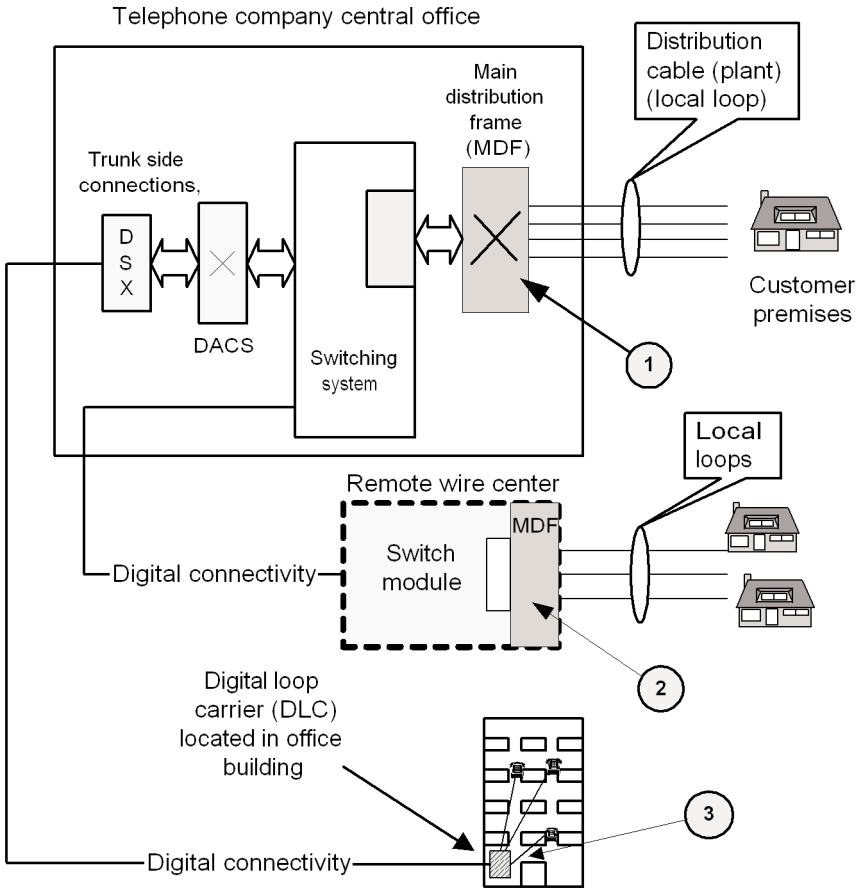


Figure 1.1. Pen register and wiretap connection points in the telephone network.

Pen registers require what is known as a *friendly* line for access by the requesting LEA to recover collected data. The physical connections for a pen register, when installed at a telephone company mainframe, are shown in Figure 1.2. The same configuration is used for installations at remote wire centers or DLC.

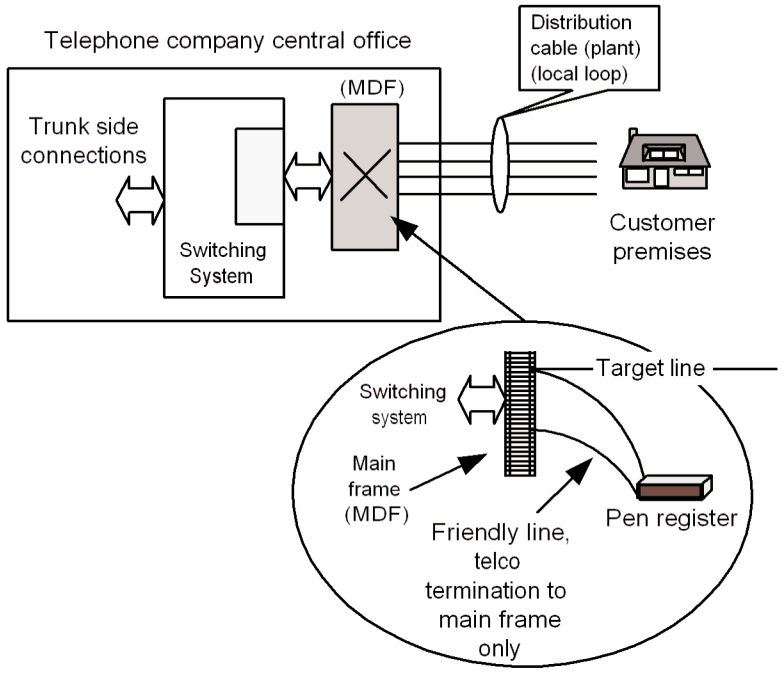


Figure 1.2. Pen register installation at telephone company mainframe

Pen registers capture dialed digits for outgoing calls and caller ID for incoming calls. Table 1.1 lists data gathered from a pen register installation.

Table 1.1. DATA GATHERED BY PEN REGISTERS

- Off-hook/On-hook times
- Hook flash times, to initiate three-way calling [conference calling] or pick up incoming calls on call waiting
- Incoming caller ID data, including caller ID on call waiting (on the assumption that the target line has caller ID as a feature)
- All dialed digits including:
  - Called number
  - Calling card numbers
  - Account codes
  - PIN digits

As seen in Table 1.1, pen registers can capture dialed digits for outgoing calls past the number dialed. For example, a pen register can capture an 800 number dialed by the target line, followed by a calling